REMARKS/ARGUMENTS

Claims 1-42 are pending in this application. Claims 1-6, 12, 19, 21, and 40 have been amended. Applicants believe that no new matter is being introduced by the amendments.

Applicants gratefully acknowledges recognition of allowable subject matter in claims 11-20 and 33-39. Applicants thank Examiner Arani for the telephone interview regarding the basis of rejection for claims 40-42. It was agreed that Applicants would address a Section 112 rejection in claim 40.

Claims Rejections – 35 USC § 103

Claims 1-10 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Auerbach et al., U.S. Pat. No. 5,673,316 issued Sep. 30, 1997 and further in view of Downs et al., U.S. Pat. No. 6,226,618 filed on August 1998 (issued May 2001).

Claims 1-6 have been amended to more specifically claim the invention.

Auerbach discloses a system which utilizes distribution in order to eliminate the need for security at the distribution point. In order to achieve this, Auerbach teaches a method of security through a cryptographic envelope. This envelope ensures that the content is freely distributable, but only able to be unlocked if the proper keys are obtained from the system.

Auerbach teaches that any form of digital content once packaged in a cryptolope is able to be distributed via CD-ROM, satellite, or any other means. Thus, Auerbach does not teach, or suggest a Document Server being coupled to a network. Further, for this reason, there is no need in Auerbach's system for obtaining the location of the content, as it is implied to be well-known.

Auerbach thus defines a methodology which does not enforce conditional access. It provides cryptographic security for generation of keys and guarantee of authenticity to the system user. Once a user has obtained a valid key from the Buy Server to open an envelope, there is no further requirement by the system to return to the Buy Server to obtain keys for the same content. In order to overcome this issue, Auerbach introduces the use of fingerprinting and watermarking. Once a document has been opened, the system of Auerbach ensures that the document will have been modified to indicate which key was used to open the document. In this

manner, the source of theft or tampering can be later identified. However, the system provides no means to prevent that theft.

The system of Auerbach leaves the processing of terms and conditions to an external program packaged into the cryptolope. Once this external program has been executed and the cryptolope unwrapped, the program is no longer effective at controlling the access to the digital content. It is also described by Auerbach that this program is executed at the Buy Server, not at the UPC.

Downs discloses a system in which metadata containers can be created to point to actual secure content using an external URL, since "the size of the content is typically too large to efficiently download". Downs utilizes a cryptolope system very similar to Auerbach. In fact, Auerbach is cited as prior art.

In contrast, Applicant's system does not allow content to be distributed freely. Applicant's claimed invention limits the distribution of content, thereby controlling piracy and theft and enforcing strong terms and conditions. By using a location independent identifier, the access server is able to hide the presence of the content server unless the request is authentic and authorized. Additionally, the access server can randomly select a content server from a group of servers, change that server, etc., thereby making the system less vulnerable to attack. Specifically, Applicants' system does not publish URL's in the content metadata. Instead, the system uses URN's (Uniform Resource Names). The URN is a location independent identifier that defines some object within a particular namespace. In Applicant's system, a namespace encompasses a group of users, access servers and content servers. Applicant's system transforms the URN into a URL only if the security token presented by the client requesting an application is authentic and passes a licensing or authorization check. Thus access to actual content is controlled to only those user's who have the rights to the content.

Additionally, in the system of Downs, URLs are used in the Metadata SC, as it is the Content Provider who distributes the actual Content SC to a hosting site. Once this operation has been done, the Content SC is available at fixed locations identified by the URL in the Metadata. If the location is to change, new Metadata SCs must be created to ensure the integrity of the system.

Further, the systems of both Auerbach and Downs rely solely on cryptographic means for content protection. Once the content has been opened in the methods of Auerbach, it is only watermarked. In the system of Downs, the Player Application or UPC is responsible for re-scrambling the content before storing it onto the client computer. The scrambling key is generated by the UPC and stored hidden on the computer. In both of these cases, once the content has been downloaded, the UPC has become operatively decoupled from the network, no longer requiring any interaction with any component, whether it is a Buy Server, Clearinghouse, Content Site, or otherwise. Also, in both systems, the key used to unlock the content in itself has no implied lifetime. For this reason Downs cites the need for destroying the key used to unlock the content and creating an additional scrambling key. In contrast, in Applicant's system, the keying information is created in the form of an activator that explicitly embodies the concepts, for example, of uniqueness per unit of time, client, user, and execution.

Further, in Applicant's system, the digital signature of the access server is not used to open the cryptolope provided by the content server. The signature is used by the content server to verify that the specific request presented for a cryptolope has been properly authorized by the access server, to meet, for example, the criteria of time, client, user, and execution. This additional step is used to secure the access to the cryptolope or its parts. Thus, the content server can ensure that both the client and the access server have authentically allowed access to the content, but in no way has any means to assure that the content can be opened or used in any way.

Auerbach teaches that a control part may be the price matrix. However, the time dependency of this price matrix can only be construed to be applicable for the date and time of the transaction, not a duration or time period. A "time-limited special offer" implies that if the item is purchased during an interval, the pricing is different. It does not imply that the license is restricted to a time period. This is left to the actual execution of the control part corresponding to the terms and conditions on the Buy Server. Auerbach does not teach a method that restricts access to distribution of the content by a document server based on the terms and conditions. Once the cryptolope has been opened, Auerbach does not teach a method to restrict access to its contents.

Additionally, the system of Downs does not teach the invention of claim 3 either. Once a License SC has been generated by the Clearinghouse, a client will have access to the Content Hosting Site. In column 70, lines 6-14 Downs shows that a database is kept by the Content Hosting Site of the material that has been downloaded. The database is checked to ensure that the client only can access each piece of content one time to prevent Denial of Service attacks or unauthorized downloads. Downs does not teach restricting access for a time period as specified by the Clearinghouse. This reinforces that the system's of Downs and Auerbach are designed to distribute content and manage the access to that content from the client computer through watermarking, fingerprinting, local encryption, etc. In contrast, Applicant's claimed invention mediates access to content by coupling the client to both the content server and access server.

Applicants believe claims 1-10 are in condition for allowance.

Claims Rejections – 35 USC § 101

Claims 21-31 have been rejected under 35 U.S.C. § 101 as claiming the same invention as that of claims 5-12 of prior U.S. Patent No. 6,763,370.

Claim 21 has been amended, and Applicants believe that claims 21-31 do not claim the same invention as that of claims 5-12 of prior U.S. Patent No. 6,763,370.

Claims 40-42

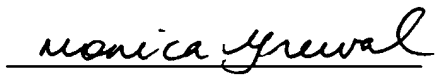
Applicants have amended claim 40 to more clearly and specifically claim the embedding of cryptographic data.

CONCLUSION

For the reasons stated above, we believe that all the claims are allowable and therefore ask the Examiner to allow them to issue.

Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,



Monica Grewal
Attorney for Applicant
Reg. No.: 40,056
monica.grewal@wilmerhale.com

Date: March 21, 2005

WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
Tel: (617) 526-6223
Fax: (617) 526-5000